كيف نصنع Trainer (حلقة 2)

رأينا في الدرس السابق كيفية صنع Trainer بسيط ثم كيف نصنع Trainer متقدم، ولكن تلك الطريقة لن تمكننا من صنع Trainers لألعاب كثيرة! هناك العديد من العوائق التي تواجه صانعي الـ Trainers، ولكن يجب عليك أن تعلم أن كافة صانعي الترابنر في العالم مستعدون لمساعدتك، ولكن بالنسبة لك كمبتدئ نرجو أن تقوم ببعث بريد إلكتروني لمجلتنا لتشرح لنا مشكلتك ومن ثم سوف نقوم بمساعدتك!! (ask@f1-mag.com)
والآن بعودتنا إلى كيفية صنع الـ Trainer نود أن تعلم أننا سوف نحاول أن نناقش كافة المشاكل التي تواجه صانعي الـ Trainers، ولكننا لن نتمكن من سردها طبعاً في درس واحد!!!

كيفية كسر الـ DMA:

ما هو الـ DMA ؟

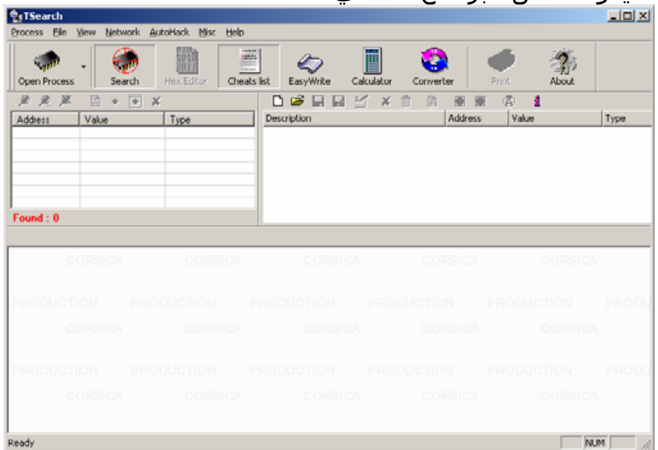
الـ DMA هو اختصار للـ Dynamic Memory Allocation أو توزيع الذاكرة الديناميكي، إذا كنت قد حاولت بالطريقة التي تعلمتها بالدرس السابق أن تصنع Trainer لألعاب أخرى مثل (Need For Speed Most Wanted) مثلاً فإنه عند بحثك عن عنوان الذاكرة الذي يتم فيه خزن قيمة النقود التي تجمعها خلال اللعب سوف تجد العنوان بالطريقة العادية ومن ثم سوف تقوم كما تعلمنا بتغيير القيمة التي يحملها هذا العنوان إلى 99999 $ مثلاً ولكن إذا حاولت أن تعيد تشغيل اللعبة سوف تجد أن الـ Trainer الذي صنعته لم يعد يعمل!!!! إذا لقد ذهب عملك سدأً، وإن ظننت أن اللعبة تحمل عدداً محدداً من العناوين لتخزين قيمة النقود فسوف تكون مخطئاً
فما هو عمل الـ DMA في الألعاب إذا؟
كما تعلم أن أغلب الألعاب الحديثة تستحوذ على حجم كبير من الذاكرة، وقد قام مبرمجوا الألعاب بإضافة هذه الميزة إلى الألعاب لكي يقللوا من الذاكرة التي تحجزها اللعبة ولكي تصبح أسرع، في الواقع إن هذه الميزة تختلف في طريقة حجز الذاكرة فكما ذكرنا أن الألعاب عند تشغيلها تحجز قسماً من الذاكرة، ولكن ما فائدة هذه الذاكرة إذا كانت اللعبة لن تستخدم إلا ستة أو سبعة عناوين (أثناء اللعب طبعاً)!! بالطبع سوف يقوم هذا الأمر بتبطيئ الحاسب، ولذلك فإن عمل الـ DMA هو حجز عنوان من الذاكرة متى ما احتاجت الى ذلك اللعبة (أي أن العنوان لا يحجز حتى تطلب اللعبة ذلك)، أعتقد الآن أن سبب عدم عمل الـ Trainer الذي صنعته عند إعادة تشغيل اللعبة أصبح واضحاً!! إن السبب في ذلك هو أنه من الممكن أن اللعبة قد طلبت عناوين أخرى قبل العنوان الذي سوف تحجزه لوضع قيمة النقود، وبالطبع مع لعبة ضخمة مثل Need For Speed Most Wanted سوف يصبح هذا الأمر معقداً جداً.
فما العمل إذا!!!! هل هذا يعني أنه يتوجب علينا إيجاد العنوان كل مرة نلعب اللعبة!!
بالطبع لا! فلو كان هذا الأمر صيحاً لم كان لهذه الدرس من فائدة ☺!!

البداية:

سوف تتعلم طريقة كسر الـ DMA عن طريق مثال، سوف نصنع في هذا المثال ترابنر للعبة Commandos Strike Force وهي لعبة حديثة وضخمة، لن نصنع ترابنر لخط الحياة هذه المرة بل لعدد الطلقات أو السكاكين التي يمكنك رميها على الأعداء.

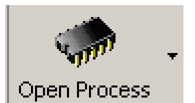
الأدوات التي سوف تحتاجها:
بعد أن قطعنا خط المبتدئين سوف نقوم بترك برنامج Game Expert لأننا الآن في هذه المرحلة سوف نحتاج الى المزيد من القدرات في برنامج البحث عن العناوين، لذلك سوف نستخدم برنامج tSearch (يمكنك أن تستخدم برنامج Cheat Engine، ولكننا في هذا الدرس سوف نستخدم برنامج tSearch، وقد قمنا بوضع البرنامجين في القرص المرفق)

بدء العمل:
بعد أن تشغل برنامج tSearch سوف يكون شكل البرنامج كالتالي:

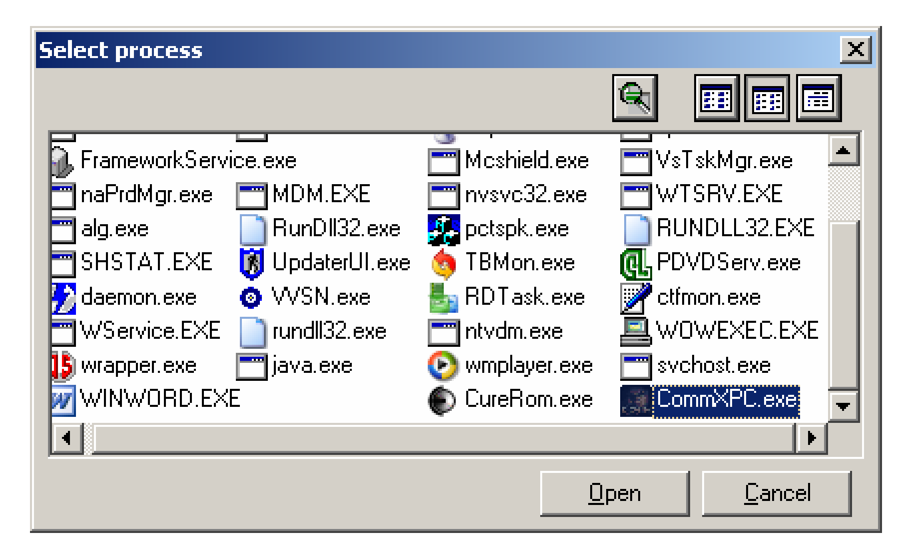


ثم قم بعد ذلك بتشغيل لعبة Commandos Strike Force (أنصحك بوضع اللعبة على أقل دقة عرض حتى تصبح عملية البحث أسرع) بعد البدء باللعب سوف تكون اللعبة كما يلي:

الآن وبعد أن عرفنا أي قيمة سوف نقوم بتثبيتها، يمكننا العودة الى برنامج TSearch باستخدام Alt + Tab ومن ثم نضغط على الزر التالي

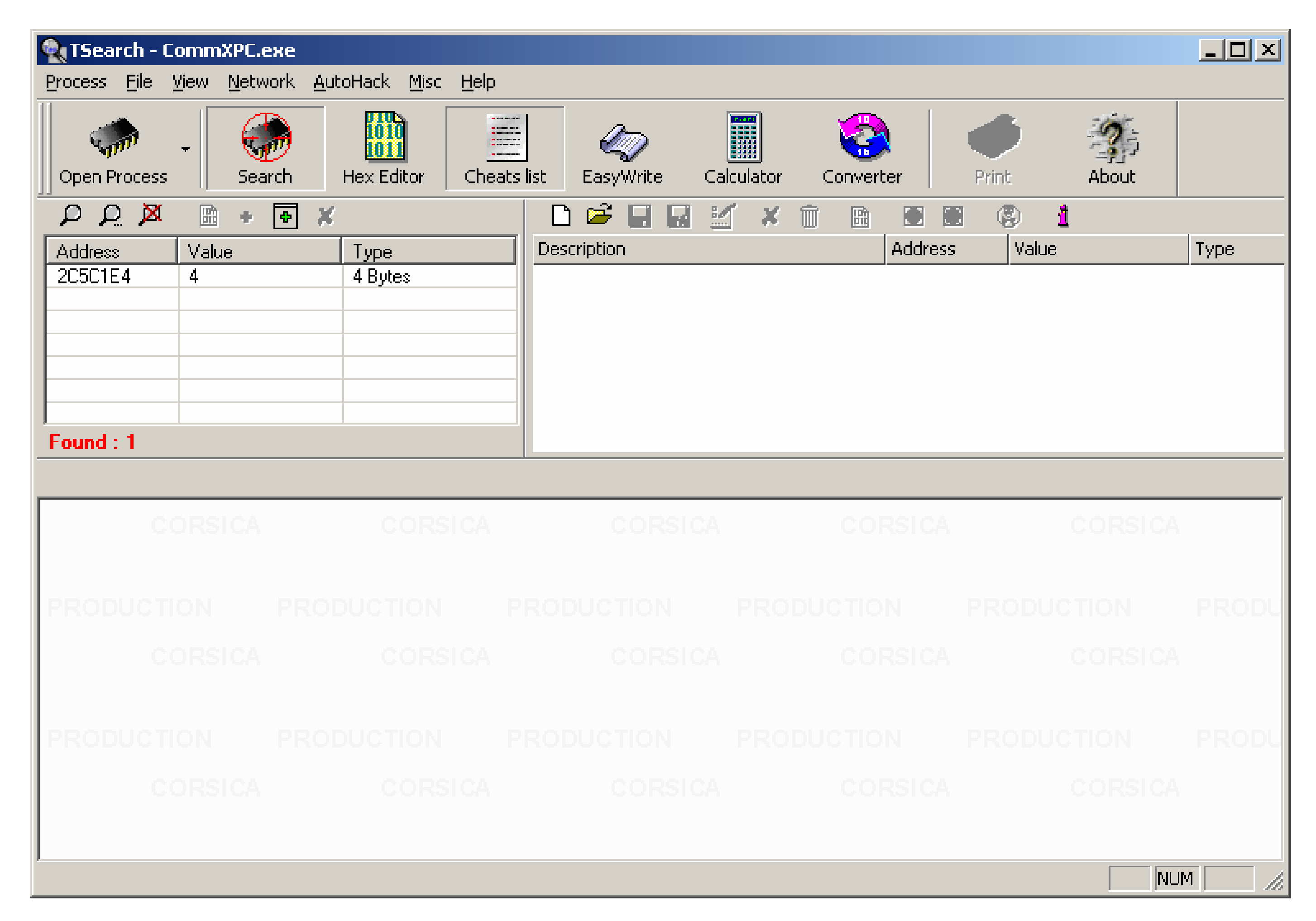


فتظهر لنا نافذة مليئة بأيقونات وأسماء البرامج التي تعمل في هذه اللحظة، نختار من هذه القائمة اسم اللعبة وهو CommXPC.exe ثم نضغط على زر Open:



نلاحظ الآن أن اسم البرنامج قد ارتبط بلعبتنا، بعد ذلك تبدأ عمليتنا بالبحث عن العنوان الذي تقوم اللعبة بتخزين قيمة عدد السكاكين فيه، نضغط على الزر الذي شكله مثل المكبرة ، ومن ثم تظهر لنا نافذة نختار من قائمة Search الموجودة في الأعلى Extract Value وفي مربع Value نضع قيمة 6 ونضبط مربع Type على 4 Byte، ومن ثم نقوم بالبحث، بعد الإنتهاء نضغط زر

OK ثم نعود الى لعبتنا وننقص عدد السكاكين برمي أحدها، ومن ثم نعود الى برنامج TSearch ونضغ على الزر الذي بجانب المكبرة وهو بنفس الشكل ولمكن تحت المكبرة يوجد خط، ثم نقوم بضغط زر OK بنجد أن عدد العناوين التي وجدها البرنامج، وبتكرار العملية السابقة مرّة أخرى فسوف نجد أنه لا يوجد سوى عنوان واحد:



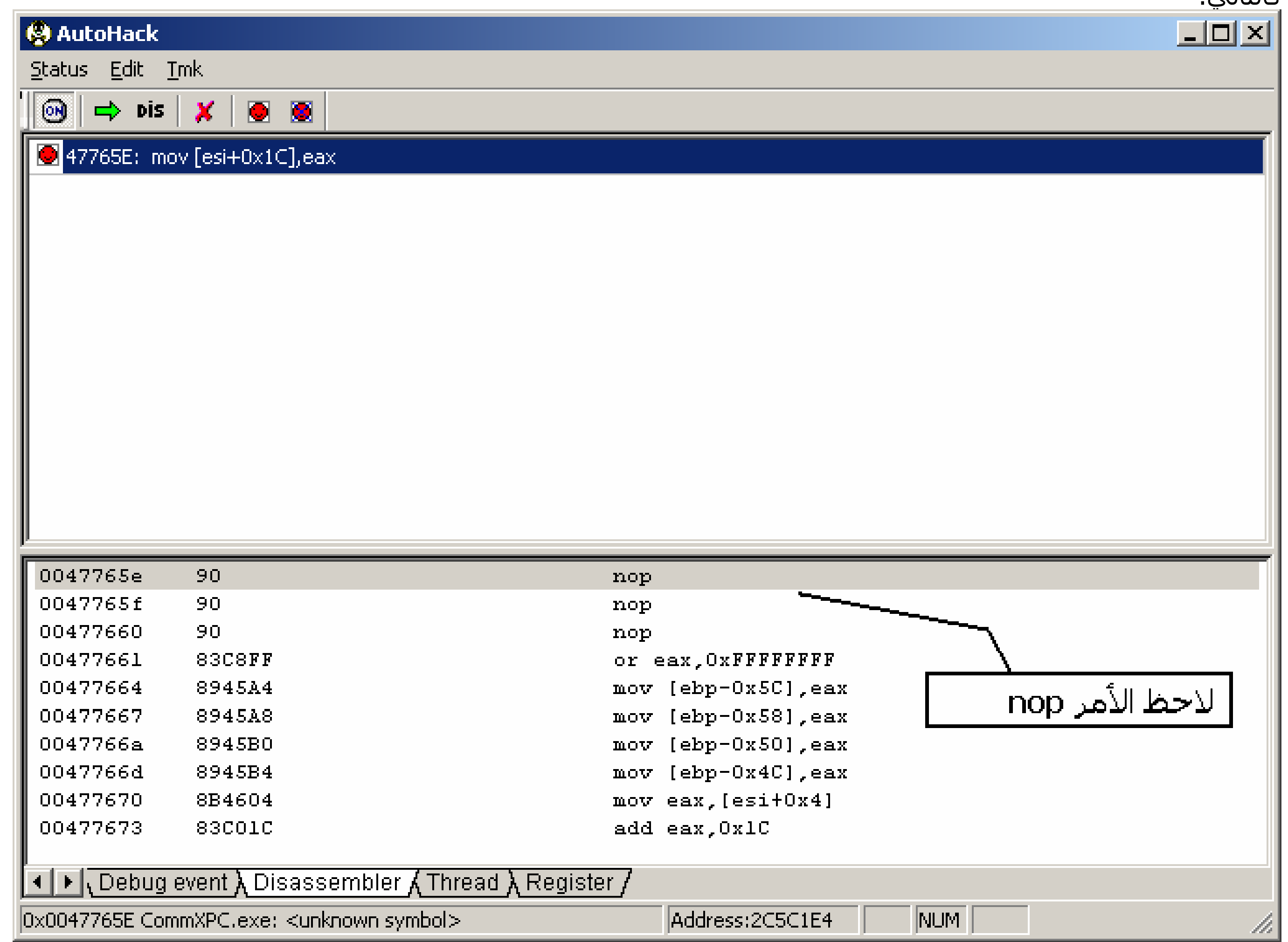
فنضغط عليه مرتين بالزر الأيسر للفأرة، فنجد أن هذا العنوان قد تمت إضافته الى القائمة الموجودة في يسار البرنامج، لكي تتأكد أن هذه هو العنوان يمكنك تغيير القيمة Value الى أي رقم تريد وليكن 15 مثلاً ثم عد الى اللعبة فتجد أن عدد السكاكين قد أصبح 15 مثل الرقم الذي اخترت، إن العنوان الذي وجدته أثناء بحثي هو: C5C1E42 ولكن العنوان الذي سوف يكون احتمال اختلافه 99%، والآن إذا قمت بإغلاق اللعبة وإعادة فتحها من جديد سوف تجد أن العنوان الذي وجدته لم يعد يعمل، بل يجب عليك أن تعود وتبحث من جديد، ومن هنا تبدأ عملية كسر الـ DMA التي تحدثنا عنها في بداية الدرس.

البدء بكسر الـ DMA:

يجب تطبيق هذه الخطوات مباشرة بعد إيجاد العنوان، أي قبل إغلاق اللعبة وإلا فلن تعمل.
من قائمة AutoHack في الأعلى اختر أمر Enable Debugger، ومن ثم اختر AutoHack Window، فتظهر لك نافذة اخرى، عد الى النافذة السابقة وقم بتحديد العنوان الذي وجدته من القائمة اليسرى ومن ثم اضغط الزر الأيمن عليه واختر AutoHack، والآن عد الى نافذة AutoHack فسوف تجد في أسفل هذه النافذة عبارة: Address: ADDR حيث تكون ADDR هي العنوان الذي وجدته، والآن عد الى اللعبة، وقم برمي أحد السكاكين مرّة أخرى وقم بالعودة مباشرة (أي قبل أن تقوم بأي شيء) الى نافذة AutoHack، فتجد أن هناك سطر قد تمت إضافته، وهو:

47765E: mov [esi+0x1c], eax

يجب أن يكون هذا السطر هو نفسه السطر الذي ظهر لك. إنّ هذا السطر هو السطر البرمجي بلغة الأسـمبلي الـذي قـوم بإنقـاص عدد السكاكين، وتنحصر مهمتنا نحن هنا بأن نقوم بإيقاف اللعبة عـن تنفيـذ هـذا الـسطر البرمجـي عـن اسـتدعاءه أي يجـب علينـا تحويل تعليمات هذا السطر الى الأمر nop أي no operation وه الأمر الذي تستخدمه لغة الأسمبلي لأمر لا يفعل أي شيء، ولكي نقوم بهذه الخطوة نقوم بالضغط على المربع الموجود علـى يـسار الـسطر الـسابق، فـنلاحظ أن هـذا المربـع قـد امـتلأ بوجـه أحمـر، كالتالي:



والآن إذا عدت الى اللعبة وحاولت أن ترمي سكينة، فسوف تجدها لاتنتي، كذلك الأمر بالنسبة لباقي الأسلحة ☺.

والآن بقي لدينا أمر واحد في هذا الدرس وهو كيفية تحول هذا الخطوات في هذا البرنامج لكـي نطبقـا فـي برنـامج Game Trainer Studio الذي علمنا أنه يمكننا من صنع Trainer على شكل ملف تنفيذي، ولكي نقوم بهـذا نختـار الـسطر الـسابق، ومـن ثـم نقـوم باختيار أمر Button Script من قائمة Tmk في أعلى البرنامج، إن هذا الـزر مخـصص فـي الأسـاس للاسـتخدام مـع برنـامج آخـر هـو Trainer Making Kit ولكن هذا البرمج يصنع Trainers بأحجام كبيرة (حوالي نصف ميغا) أما برنامج Game Trainer Studio فإنه يقوم ببناء Trainers صغير الحجم، ولكن لحسن الحظ فإن السطور البرمجية التي يـستخدمها البرنـامجين هـي نفـسها (باسـتخدام الأمـر Poke الذي تعلمنا في الدرس السابق)

والآن لكي نتعلم كيفية كتابة هذا السطر بدون استخدام الزر السابق (أي زر الـ TMK) يجب عليك أن تكون خبيراً بنظام العـد الـست عشري، للبدء يجب عليك أن تضغط مجدداً على المربع بجانب السطر السابق لكي يعود أبيضاً كما كان، ومن النافذة الـسفلية تجـد الكود بلغة الأسـملي لماقبل وما بعد هذا السطر وما يهمنا هو مابعد، لاحظ أنه على يسار سطرنا الموجود في الأسفل سـوف تجـد العدد: 0047765e، وسوف تجد على يسار السطر الذي يليه العدد: 00477661 والآن ما يجب علينا فعله هـو طـرح الـرقم الأول مـن الرقم الثاني باستخدام الآلة الحاسبة المرفقة مع ويندوز ولكن بعد ضبطها على الإسـتخدام Hex أو الـست عـشري، فنجـد أن نـاتج عملية الطرح في مثالنا هذا هو 3 وهذا يدلنا أنه لكي نقوم بتعديل الـسطر الـسابق يجـب أن نبـدل كـوده بتعليمـة nop علـى ثلاثـة أسطر يكون هو أولها وتعليمتي الـ nop الأخريتين يجب أن تكونا على السطور التي بعده أي أن تصبح السطور الثلاثة كما يلي:

هذا السطر هو السطر الذي توجد عليه التعليمة الأساسية

0047765e 90 nop →

حصلنا على على عنوان هذا السطر من خلال إضافة 1 الى العدد الست عشري السابق

0047765f 90 nop →

حصلنا على عنوان هذا السطر بنفس العملية السابقة

00477660 90 nop →

أما بالنسبة للرقم 90 فهو مايقابل التعليمة nop بطريقة البرمجة الست عشرية (حيث أنه لا يوجد فقط نظام أرقام ست عشري، بل بإمكانك تحول تعليمات الأسمبلي الى النظام الست عشري أيضاً)

وبالنسبة الى السطر الذي يجب علينا إضافته الى برنامج الـ Game Trainer Studio فسوف يكون بحسب تعليمة Poke كما يلي Poke (عنوان السطر الأساسي) 90 90 90

أي:

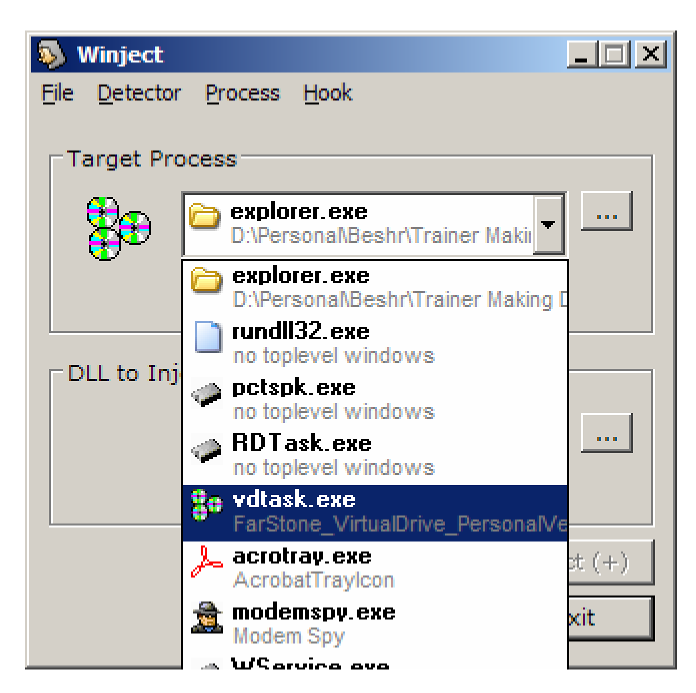
Poke 0047765e 90 90 90

وبإضافة هذا الأمر الى وظائف أحد الأزرار في برنامجي Game Trainer Studio في إثناء التصميم فسوف يقوم الترainer الذي صنعناه بتعطيل هذا الأمر ولن تنقص عدد السكاكين أو الرصاصات بعد الآن.

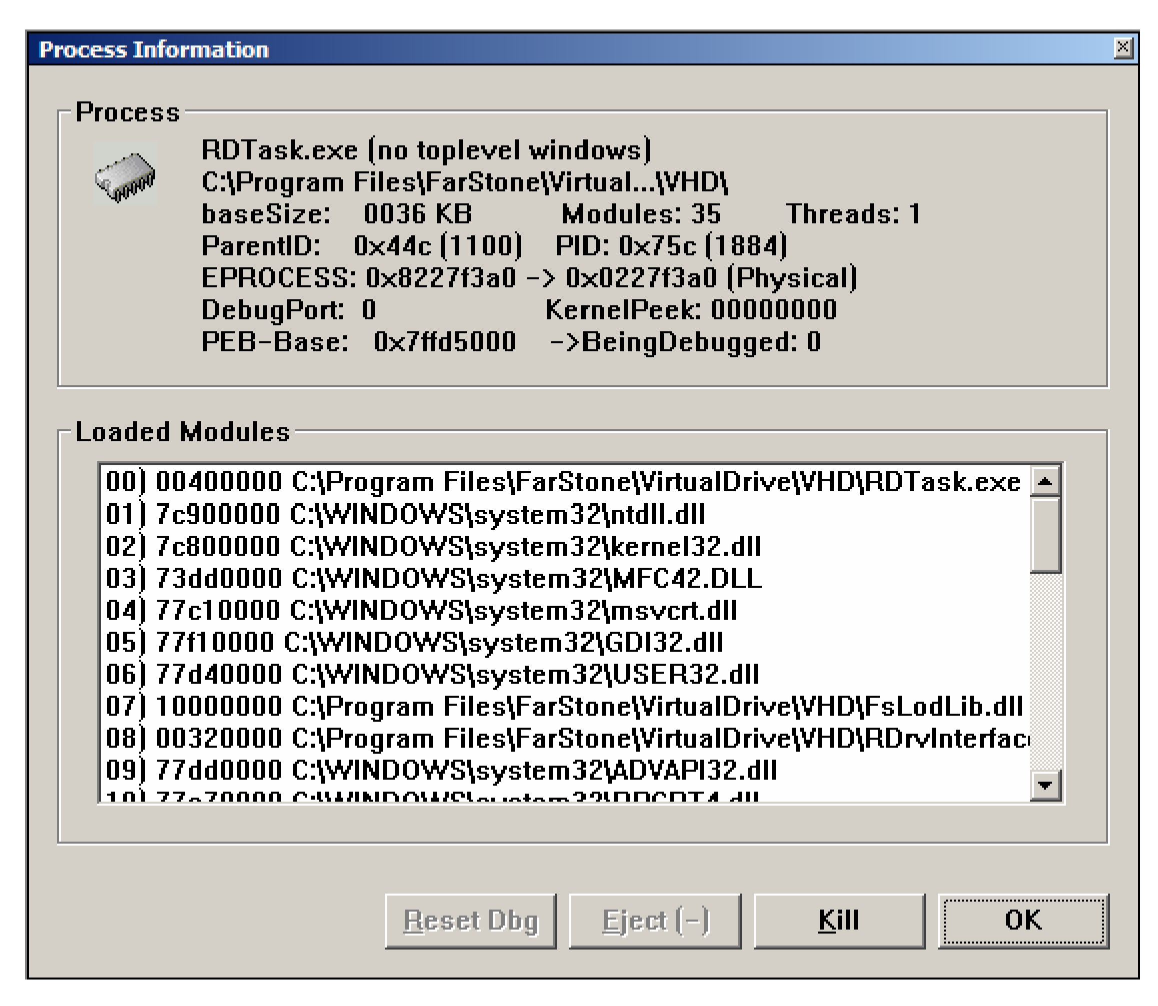
بالطبع يمكن أن تقوم بتطبق هذه العملية نفسها على خط الحياة في بعض الألعاب (لا يمكنك ذلك في لعبة Commandos Strike Force، لأنها تستخدم غير طريقة) كما أنه يجب عليك أن تعلم أن هذه الطريقة والطريقة التي تعلمناها في الدرس السابق لا تكفينا لصنع Trainer لجميع الألعاب، وكما لاحظت في هذا الدرس أننا استخدمنا قليلاً من علم لغة الأسملبي، فيتوجب عليك أن تبدأ بتعلم القليل من لغة الأسمبلي قبل البدء بالدرس التالي لأننا سوف نستخدم تعليمات الأسمبلر بكثرة.

ملاحظات على هذا الدرس:

1. كما لاحظت أننا قمنا بإضافة Debugger لهذا اللعبة، فسوف تلاحظ أنه في بعض الألعاب أن الـ Debugger يكون موجوداً في اللعبة في الأساس، ولهذا لن يكون بإمكاننا من إضافة الـ Debugger الموجود في برنامج tSearch ولكن لا تخف فإن لهذه المشكلة حل، وهو برنامج Winject17b وهو برنامج مصمم لعملية حقن الأكواد في داخل برنامج اللعبة (سنتكلم عن هذا الأمر في دروس أخرى) ولكن سوف نستفيد من هذا البرنامج في درسنا هذا فقط في عملية اخراج الـ Debugger من اللعبة، ولكي نقوم بهذا الأمر نقوم بتشغيل البرنامج ثم من قائمة Target Process نختار اللعبة التي نريد أن نخرج الـ Debugger منها، كما في الشكل:



بعد ذلك نضغط على الزر بجانب هذا المربع، والذي يحمل الاسم (...) فنلاحظ ظهور مربع الحوار التالي:



فإذا كانت اللعبة تحتوي على Debugger فنلاحظ أن الزر الذي يحمل الاسم Reset Dbg قد أصبح مفعلاً ووظيفة هذا الزر هي إلغاء الـ Debugger من اللعبة (إذا كانت تحتوي عليه) لكي نتمكن من إذافة الـ Debugger الخاص بنا.

2. لقد قمنا بإضافة الـ Trainer الذي تعلمنا صنعه في هذا الدرس مع القرص المرفق.

بشر كيالي
tRAINER2006